

ENTERED

November 03, 2022

Nathan Ochsner, Clerk

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

KONNECH INC.,

Plaintiff,

VS.

TRUE THE VOTE INC., *et al.*,

Defendants.

§
§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. 4:22-CV-03096

**MEMORANDUM OPINION AND ORDER ON
MOTION FOR A PRELIMINARY INJUNCTION****I. INTRODUCTION**

Before the Court are the plaintiff's, Konnech, motion for a preliminary injunction and brief in support [DE 5] and the defendants, True the Vote, Inc., Gregg Phillips and Catherine Engelbrecht's, opposition to Konnech's motion [DE 24]. The parties submitted the matters to the Court on the evidence and arguments presented in open court. After a careful review of the motion and response and the affidavit provided by Konnech, the Court determines that a preliminary injunction should be entered.

II. FACTUAL BACKGROUND

Konnech brings this suit for injunctive relief and damages based on allegations that the defendants violated the federal Computer Fraud and Abuse Act, [Title 18 U.S.C. § 1030 *et. seq*] and the Texas Harmful Access by Computer statute also codified in the Texas penal code, [Tex. Civ. Prac. & Rem. Code § 143.001; Texas Penal Code § 33.02, respectively].

Konnech is a domestic corporation, incorporate in the state of Michigan, that contracts to provides governmental entities throughout the United States with technical assistance and software that enables the governmental entities to recruit, train and schedule poll workers, coordinate the distribution of equipment and supplies to polling places, and to dispatch support personnel to address technical and other issues related to staffing, security and the handling of ballots. Konnech's contractual duties do not include the registration of voters, the production, distribution, scanning, or processing of ballots; nor does it collect, count or report votes. Indeed, because Konnech does not handle ballots, it does not enter balloting data onto its computer servers.

Finally, the evidence shows that Konnech acquired its contracts with governmental entities through public government bidding processes. Therefore, all of the data acquired and held by Konnech was acquired from the governmental entities it serves. Hence, the workers' data is personal and confidential and is secured exclusively on protected computers located in the United States. The software program created by Konnech for polling purposes, [the Poll Chief], is a product created for governmental entities to conduct their election polling responsibilities.

III. CONTENTIONS OF THE PARTIES

A. Konnech's Contentions

Konnech contends that on several occasions the defendants and others unknown to Konnech hosted an "event" dubbed "The Pit" podcast in August 2022, where the defendants claimed that they would disclose information acquired from Konnech's

computer servers that would constitute proof that the 2020 Presidential Election was stolen from former President Donald Trump. The event featured multiple speakers and the defendants' announcement of a website that they had created or was in the process of creating, for the purpose of displaying the evidence gathered, which evidence, would prove election fraud.

Konnech contends that following The Pit event, the defendants posted messages on social media that defendant Phillips, "and his guys", had successfully hacked into Konnech's servers and downloaded Konnech's data. The defendants also alleged that they had met with, or turned over to FBI agents their findings and that they would, nevertheless, soon post Konnech's data on their new website.

Konnech asserts that the defendants have accused Konnech and its founder, Eugene Yu, of being a "Chinese operative, spearheading a 'Red Chinese communist op run against the United States.'" Konnech also asserts that the defendants have publicly accused Yu of acts of treason, espionage, bribery and election fraud, all for the purpose of enriching themselves based on a racist and xenophobic conspiracy designed to harm Konnech's business and its founder's reputation.

As a result of these allegations, Konnech seeks a preliminary injunction and asserts the following state and federal claims in its lawuist: (1) defamation, libel and slander; (2), tortious interference with existing and prospective business relations; (3), violating the Computer Fraud and Abuse Act, (18 U.S.C. § 1030); (4), conspiracy to violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (5 and 6), computer conspiracy to gain

harmful access by computer (Tex. Civ. Prac. & Rem. Code, § 143.001 and Texas Penal Code § 33.02); (7), Conversion; (8), violation of the Texas Theft Liability Act (Tex. Civ. Prac. and Remedies Code, Chapter 134); and, (9), injunctive relief, damages, attorneys' fees and costs of suit.

B. The Defendants' Contentions

The defendants contend that True the Vote is a nonprofit organization that, since 2009, has worked to support election integrity. "Its mission is to promote the security and integrity of the voting process." The defendants have "deep concern[s] about the intervention by the People's Republic of China in United States elections."

In a series of contentions, the defendants make the following assertions: (1), Konnech has falsely accused the defendants of racism and xenophobia against Yu and the government of China; (2), Konnech also has falsely accused True the Vote of having "peddled" claims of election fraud to "enrich" and "profit" itself; (3), True the Vote's requests, under the Freedom of Information Act, to obtain "public documents from various governmental entities" do not constitute a violation of federal or state law; (4), True the Vote has identified "a key document" that supports its (public domain) statements that also shows up on Konnech's website; (5), Konnech's pleadings, affidavit and exhibits fail to demonstrate that its computers were hacked; (6), Konnech has failed to properly assert its two conspiracy claims against the defendants in that they are merely agents of True the Vote, and a corporation cannot conspire with itself. This is so because their acts are the acts of the corporation.

As to the federal and state claims that the defendants hacked Konnech's computers, the defendants assert that they did not violate the statutes. They accessed a server in China and acquired the data for a Chinese computer, therefore, the defendants contend, Konnech is not entitled to a preliminary injunction.

IV. DISCUSSION AND ANALYSIS

The Federal Rules of Civil Procedure, Rule 65 addresses the circumstances under which a TRO and preliminary injunction may issue. A TRO may be issued without written or oral notice where:

- (A) specific facts in an affidavit or verified complaint show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and,
- (B) the movant's attorney certifies in writing any efforts made to give notice and the reasons why it should be required.

FRCP, Rule 65. A motion for a preliminary injunction must, however, be set for hearing at the earliest possible date, at which time, the Court must proceed with the motion. *Id.* at 65(3).

In the case at bar the attorneys for both parties entered into a stipulation agreeing that the TRO, that was entered by the Court, would continue in effect until the Court either dissolves the TRO or enters a preliminary injunction. The parties also agreed that Konnech's motion for a preliminary injunction may be submitted to the Court on the papers of the parties since none of the parties were present in Court.

A motion for a preliminary injunction is governed by Federal Rules of Civil Procedure, Rule 65 which requires that a movant shows that he will suffer irreparable injury

if an injunction is not granted; there is relatively little or no harm visited on the non-movant by the issuance of an injunction; the public interest is not harmed by the issuance of an injunction; and the movant will likely prevail on the merits of his lawsuit. *Daniels Health Sciences, L.L.C. v. Vascular Health Sciences, L.L.C.*, 710 F.3d 579, 582 (5th Cir. 2013).

Konnech's suit asserts claims against the defendants in common law and under Texas and federal statutes. Konnech asserts that the defendants have, by their admissions concerning data in their possession, that they claim they acquired from a Chinese server, admit that they are in possession of data that belongs to Konnech. This data, whether acquired from Konnech or China, is personal and confidential to Konnech and the poll workers of the various counties and States in the United States where the workers are employed. The defendants describe their acquisition of this data as follows:

Gregg and Catherine, gc, stumble onto voting software used to coordinate elections was left with default password or database. GC research team discovered sensitive information on election workers, etc. on server (bank account info, kids' names, ssn etc-gc takes to fbi . . .

In order to establish a *prima facie* violation of the federal Computer Fraud and Abuse Act, a plaintiff must present evidence that a defendant has intentionally accessed a protected computer; without authorization or has exceeded authorized access; the defendant obtained and possesses the information or data and, the plaintiff will suffer damages or loss of at least \$5,000. *See* Title 18 U.S.C. § 1030 (c)(4), (e)(1 and 2)(b-c).

The State of Texas, in addressing alleged unauthorized access under state law, couples unauthorized access to another's computer with section. 33.02(a) of the State Penal Code. There, the Code and defines access as communicat[ing] with, stor[ing] data in,

retri[ing] or intercept[ing] data . . . from another's computer without prior authorization. *See* Tex. Civ. Prac. & Rem. Code § 143.001; Texas Penal Code § 33.02(a).

In accessing Konnech's computer and/or collecting, storing or retrieving data known to belong to Konnech, the defendants have interfered with Konnech's lawful right to control its own computers and data, and, moreover, protect the personal and confidential data of individuals who serve as "poll workers".

The evidence shows that Konnech provides governmental entities in the United States with an election logistics software, called Poll Chief, that is used by the governmental entities to recruit, train and schedule poll workers, including other polling duties. On or about August 13, 2022, the defendants announced that they were engaged in an attack against Konnech, claiming that Konnech and its President, Eugene Yu, were Chinese operatives working for the Chinese Communist Party to interfere with elections in the United States.

Since the August event, Yu asserts, without challenge, that he and his family have been personally threatened. Moreover, Konnech and Yu are under threats as a result of the defendants' media events, whereby they announced their intent to release to the public all of the data that they acquired from Konnech's protected computers. To do so, in the Court's opinion, would destroy trust in the governmental entities by the public and, trust between the governmental entities and Konnech. *See* [Affidavit Attached to Motion for TRO and Preliminary Injunction, DE 5-1]. Therefore, the Court is of the view that Konnech has demonstrated facts that support the issuance of a preliminary injunction.

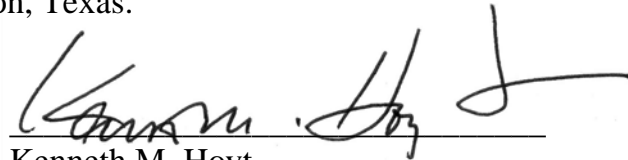
In response, the defendants have filed an unsworn written response. And, except for taking issue with whether they “hacked” Konnech’s computers, they do not deny the assertions stated in Yu’s affidavit. Therefore, the Court finds that a *prima facie* case is established by the documents and record, that the defendants gained unauthorized access to Konnech’s or another’s computer(s) and obtained personal and confidential data that is stored on Konnech’s computers. Hence, the defendants are interfering with Konnech’s control over its protected computer data to the detriment of Konnech, the governmental entities and their employees.

Therefore, it is ORDERED that a preliminary Injunction issues, ENJOINING the defendants, their agents and assigns:

- (i) from accessing or attempting to access Konnech’s protected computers;
- (ii) from using, disclosing, or exploiting the property and data downloaded from Konnech’s protected computers; and further, they are;
- (iii) ordered to identify each individual and/or organization involved in accessing Konnech’s protected computers;
- (iv) ordered to return to Konnech all property and data obtained from Konnech’s protected computers, whether original, duplicated, computerized, handwritten, or any other form, whatsoever obtained from any source;
- (v) ordered to preserve, and not to delete, destroy, conceal or otherwise alter, any files or other data obtained from Konnech’s protected computers;
- (vi) ordered to confidentially disclose to Konnech how, when, and by whom Konnech’s protected computers were accessed; and

- (vii) ordered to identify all persons and/or entities, in defendants' knowledge, who have had possession, custody or control of any information or data from Konnech's protected computers.

SIGNED on October 31, 2022, at Houston, Texas.

A handwritten signature in black ink, appearing to read "Kenneth M. Hoyt", written over a horizontal line.

Kenneth M. Hoyt
United States District Judge